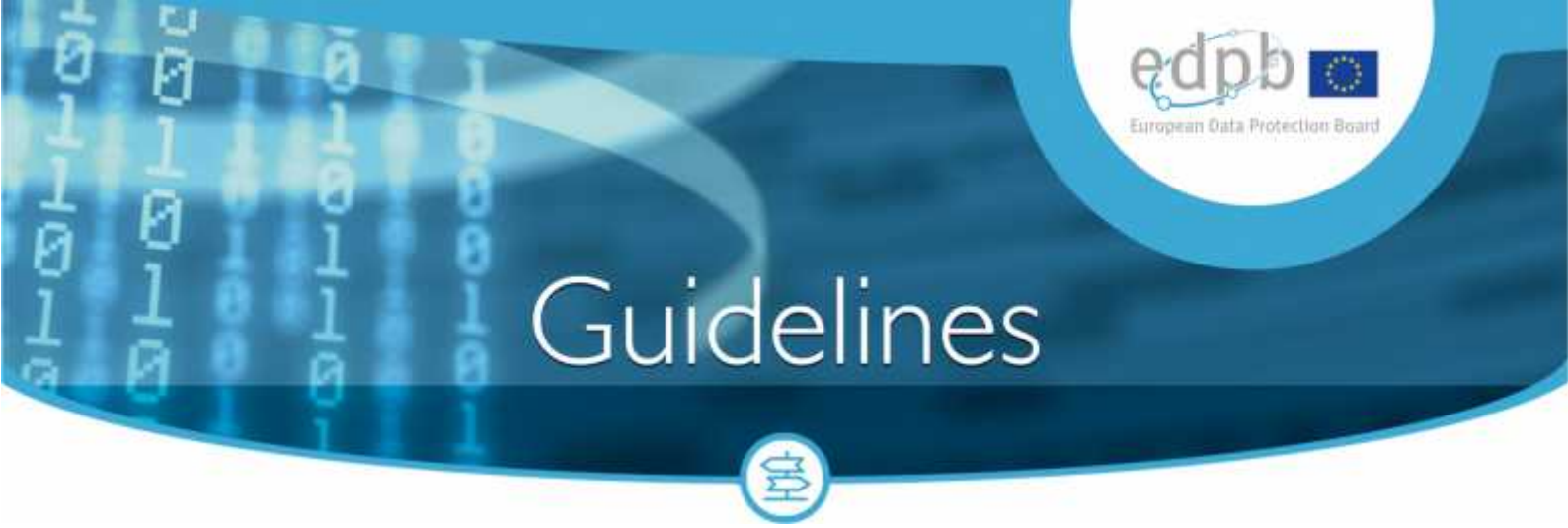

Guidelines 10/2020 on restrictions under Article 23 GDPR

Version 1.0

Adopted on 15 December 2020

Table of contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. This document seeks to provide guidance as to the application of Article 23 GDPR. These Guidelines provide a thorough analysis of the criteria to apply restrictions, the assessments that need to be observed, how data subjects can exercise their rights once the restriction is lifted and the consequences for infringements of Article 23 GDPR.

2. The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules in relation to the protection of personal data and the rules relating to the free movement of personal data. The GDPR protects the rights and freedoms of natural persons and in particular their right to data protection. Data protection cannot be ensured without adhering to the rights and principles set out in the GDPR (Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided in Articles 12 to 22 GDPR). All these rights and obligations are at the core of the fundamental right to data protection and their application should be the general rule. In particular, any limitation to the fundamental right to data protection needs to observe Article 52 of the Charter of fundamental rights of the European Union ("the Charter").

3. It is against this background that Article 23 GDPR should be read and interpreted. This provision is entitled 'restrictions' and it provides that, under Union or Member State law, the application of certain provisions of the Regulation, mainly relating to the rights of the data subjects and controllers' obligations, may be restricted in the situations therein listed. Restrictions should be seen as exceptions to the general rule of allowing the exercise of rights and observing the obligations enshrined in the GDPR[2]. As such, restrictions should be interpreted narrowly, only be applied in specifically provided circumstances and only when certain conditions are met.

4. Even in exceptional situations, the protection of personal data cannot be restricted in its entirety. It must be upheld in all emergency measures, as per Article 23 GDPR thus contributing to the respect of

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] These situations do not include the scenarios where the Law Enforcement Directive applies.

the overarching values of democracy, rule of law and fundamental rights on which the Union is founded: any measure taken by Member States shall respect the general principles of law, the essence of the fundamental rights and freedoms and shall not be irreversible and data controllers and processors shall continue to comply with data protection rules.

5. In all cases, where Union or Member State law allows restrictions to data subjects' rights or to the obligations of the controllers (including joint controllers[3]) and processors[4], it should be noted that the accountability principle, as laid down in Art. 5(2) GDPR, is still applicable. This means that the controller is responsible for, and shall be able to demonstrate to the data subjects his or her compliance with the EU data protection framework, including the principles relating to the processing of their data.

6. When the EU or national legislator lays down restrictions based on Art. 23 GDPR, it shall ensure that it meets the requirements set out in Art. 52(1) of Charter, and in particular conduct a proportionality assessment so that restrictions are limited to what is strictly necessary.

2 THE MEANING OF RESTRICTIONS

7. The term restrictions is not defined in the GDPR. Article 23 and Recital 73 GDPR only list the conditions under which restrictions can be applied.

8. In these guidelines, the term restrictions will be defined as any limitation of scope of the obligations and rights provided for in Articles 12 to 22 and 34 GDPR as well as corresponding provisions of Article 5 in accordance with Article 23 GDPR. A restriction to an individual right has to safeguard important objectives, for instance, the protection of rights and freedoms of others or important objectives of general public interest of the Union or of a Member State which are listed in Article 23(1) GDPR. Therefore, restrictions of data subjects' rights can only occur when the listed interests are at stake[5] and these restrictions aim at safeguarding such interests.

9. Consequently, the grounds for the restriction need to be clear. To be lawful, restrictions shall be provided for in a legislative measure, concern a limited number of rights of data subjects and/or controller's obligations which are listed in Article 23 GDPR[6], respect the essence of the fundamental rights and freedoms at issue, be a necessary and proportionate measure in a democratic society and safeguard one of the grounds set out in Article 23(1) GDPR as described below.

10. In addition, as mentioned in Recital 73 GDPR, restrictions should be in accordance with the requirements set out in the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms.

11. In addition to restrictions referred to in Article 23, the GDPR also lays down provision relating to specific processing situations as per Chapter IX, where Member States may provide by law specific measures impacting data subjects' rights, such as exemptions or derogations (for instance, Articles 85 or 89 GDPR). However these guidelines do not address those cases.

[3] In case of joint controllership, especially in case where controllers are from different Member states, restrictions applicable in accordance with Article 23 should be considered and taken into account so that joint controllers clarify in the arrangement their respective roles.

[4] Although from now on the guidelines will refer to "controllers" only, the recommendations are addressed, where applicable, also to processors.

[5] These interests are exhaustively listed in Article 23 (1) GDPR.

[6] There are certain rights which cannot be restricted under Article 23 GDPR, such as the right to submit a complaint to the supervisory authority (Article 77 GDPR).

12. Restricting the scope of the obligations and rights provided for in Article 12 to 22 and Article 34 may take different forms but never reaching the point of a general suspension of all rights. Legislative measures laying down the provisions for the application of restrictions under Article 23 GDPR may also foresee that the exercise of a right is delayed in time, that a right is exercised partially or circumscribed to certain categories of data or that a right can be exercised indirectly through an independent supervisory authority.

3 REQUIREMENTS OF ARTICLE 23(1) GDPR

13. Article 23(1) GDPR lists a number of requirements, which will be detailed below. All those requirements need to be met in order for a measure to be lawfully relied upon.

3.1 Respect of the essence of the fundamental rights and freedoms

14. One of the main objectives of data protection law is to enhance data subjects' control over personal data concerning them. Any restriction shall respect the essence of the right that is being restricted. This means that restrictions that are extensive and intrusive to the extent that they void a fundamental right of its basic content, cannot be justified. In any case, a general exclusion of all data subjects' rights with regard to all data processing operations as well as a general limitation of the rights mentioned in Article 23 GDPR of all data subjects for specific data processing operations or with regard to specific controllers would not respect the essence of the fundamental right to the protection of personal data, as enshrined in the Charter. If the essence of the right is compromised, the restriction shall be considered unlawful, without the need to further assess whether it serves an objective of general interest or satisfies the necessity and proportionality criteria.

15. In order to guarantee this control, data subjects have a number of rights within the right to data protection and the controller has a number of obligations vis a vis the data subject, set out under Articles 12 to 22 and Article 34 GDPR, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22 GDPR. It is against this background that Article 23 GDPR should be read and interpreted.

3.2 Legislative measures laying down restrictions and the need to be foreseeable (Rec. 41 and CJEU case law)

16. The requirement of a legislative measure entails that controllers can only rely on a restriction provided for by Article 23 GDPR to the extent that this restriction has been specified in Union or Member state law. Without the corresponding legislative measure, controllers cannot rely directly on the grounds listed in Article 23(1) GDPR. Recital 41 GDPR states that "[w]here this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union [...] and the European Court of Human Rights"[7].

17. According to Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter shall be 'provided for by law'. This echoes the expression 'in accordance

[7] The type of legislative measures considered has to be in line with EU law or with the national law. Depending on the degree of interference of the restriction, a particular legislative measure, taking into account the level of norm, could be required at national level.

with the law' in Article 8(2) of the European Convention of Human Rights[8], which means not only compliance with domestic law, but also relates to the quality of that law without prejudice to the nature of the act, requiring it to be compatible with the rule of law. In particular, the domestic law must be **sufficiently clear in its terms to give citizens an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such restrictions**. The same strict standard should be applied for any restrictions that could be imposed by Member States. In line with the GDPR and the case law of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR), it is indeed essential that legislative measures, which seek to restrict the scope of data subject rights or of controller's obligations, are foreseeable for the data subjects.

18. While any legislative measure must in any case be adapted to the objective pursued and meet the foreseeability criterion, a legislative measure laying down the provisions for the application of restrictions under Article 23 GDPR does not always have to be limited in time or linked to a specific period.

    a. In some cases, the restriction is not specifically linked to a timeframe because the ground for the restriction to be safeguarded by the legislative measure is not in itself limited in time. In light of the principle of necessity and proportionality, it is necessary to ensure that such legislative measures relate to a ground for restriction to be safeguarded on an ongoing basis, or permanently, in a democratic society. For instance, a legislative measure restricting the scope of the obligations and rights provided for in Article 12 to 22 and Article 34, for safeguarding the protection of judicial independence and judicial proceedings may for example be considered as fulfilling a continuing objective in a democratic society and therefore may not be limited in time.

    b. In other cases, the ground for the restriction to be safeguarded is in itself limited in time and therefore the legislative measure should provide a limitation in time in order to meet the foreseeability criterion. For example, where restrictions are adopted in the context of a state of emergency to safeguard public health, the EDPB considers that restrictions, imposed for a duration not precisely limited in time, do not meet the foreseeability criterion, including when such restriction apply retroactively or are subject to undefined conditions.

19. This link between the foreseen restrictions and the objective pursued should be clearly established and demonstrated in the concerned legislative measure or additional supplementary documents. For instance, the mere existence of a pandemic alone is not a sufficient reason to provide for any kind of restriction on the rights of data subjects; rather, any restriction shall clearly contribute to the safeguard of an important objective of general public interest of the Union or of a Member State.

[8] See in particular, European Court of Human Rights, 14 September 2010, Sanoma Uitgevers B.V. v. The Netherlands, EC:ECHR:2010:0914JUD003822403, paragraph 83: "Further, as regards the words "in accordance with the law" and "prescribed by law" which appear in Articles 8 to 11 of the Convention, the Court observes that it has always understood the term "law" in its "substantive" sense, not its "formal" one; it has included both "written law", encompassing enactments of lower ranking statutes and regulatory measures taken by professional regulatory bodies under independent rule-making powers delegated to them by Parliament, and unwritten law. "Law" must be understood to include both statutory law and judge-made "law". In sum, the "law" is the provision in force as the competent courts have interpreted it". On the notion of 'provided for by law', the criteria developed by the European Court of Human Rights should be used as suggested in CJEU Advocates General opinions in joined cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, paragraphs 137-154 or in case C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, paragraph 99.

3.3 Grounds for the restrictions

20. In order to adopt a legislative measure for restrictions and to apply a restriction in a concrete case, one or several of the following conditions stated in Article 23(1) GDPR need to be met. This list is exhaustive, meaning restrictions cannot be carried out under any other conditions than the ones listed below.

21. The link between the foreseen restrictions and the objective pursued should be clearly stated in the legislative measure.

3.3.1 National security, defence and public security

22. A restriction to data subject rights can have national or public security and/or defence of the Member States as an objective to be safeguarded, as stated in Article 23(1)(a), (b) and (c) GDPR.

23. Moreover, public security includes protection of human life, especially in response to natural or manmade disasters.

3.3.2 Prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties including the safeguarding against and the prevention of threats to public security

24. In certain cases, providing information to the data subjects who are under investigation might jeopardise the success of that investigation. Therefore, the restriction of the right to information or other data subject's rights may be necessary, under Article 23(1)(d) GDPR. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories[9]

25. Nonetheless, the omitted information shall, in accordance with the case law of the CJEU, be provided once and if it is no longer possible for it to jeopardise the investigation being carried out[10]. This means that a specific (tailor-made) data protection notice should be given to the data subject as soon as possible, stating the different rights such as access, rectification etc.

26. Also, the objective of safeguarding public security includes the protection of human life especially in response to natural or manmade disasters[11].

3.3.3 Other important objectives of general public interest

27. Article 23(1)(e) GDPR mentions as other important objectives of general public interest of the Union or of a Member-State important economic or financial interest, including monetary, budgetary and taxation matters, public health and social security. It may concern for instance the keeping of public registers kept for reasons of general public interest or the further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes[12]. On the other hand, the costs incurred as a consequence of providing information and thus the financial burden on public budgets are not sufficient to justify a public interest in restricting the rights of the data subjects.

3.3.4 Protection of judicial independence and judicial proceedings

28. Article 23(1)(f) GDPR also foresees the need to restrict certain data subjects' rights or controller's obligations, in order to protect judicial independence and judicial proceedings.

---

[9] Recital 19 GDPR.
[10] Opinion 1/15 of the CJEU (Grand Chamber) on the Draft PNR Agreement between Canada and the European Union, 26 July 2017, ECLI:EU:C:2017:592.
[11] Recital 73 GDPR.
[12] Recital 73 GDPR.

29. The scope of these restrictions should be aligned with national legislation regulating these matters.

3.3.5 Prevention, investigation, detection and prosecution of breaches of ethics for regulated professions

30. Article 23(1)(g) GDPR mentions breaches of ethics for regulated professions, such as medical doctors and lawyers.

31. These are cases in which an investigation does not relate in principle with criminal offences as, where the investigation concerns a criminal offence, the ground set out under point 3.3.2 would be applicable.

3.3.6 Monitoring, inspection or regulatory function connected to the exercise of official authority in the cases referred to in points (a) to (e) and (g) of Article 23 GDPR

The ground for restriction mentioned in Article 23(2)(h) GDPR refers to a potential limitation when there is an inspection or a monitoring exercise or a regulatory function connected, even if only occasionally, to the exercise of official authority in the cases referred to in points 3.3.1 to 3.3.3 and 3.3.5.

3.3.7 Protection of the data subject or the rights and freedoms of others

32. Article 23(1)(i) GDPR refers to a ground for restriction that aims to protect the data subject or the rights and freedoms of other persons.

33. One can illustrate a restriction to protect the rights and freedoms of others with an example of an investigation where the identity of an alleged victim, witnesses or whistle-blower cannot be disclosed in order to protect them from retaliations.

3.3.8 Enforcement of civil law claims

34. Article 23(1)(j) GDPR also includes the enforcement of civil law claims as a ground for restrictions. While Article 23(1)(j) GDPR allows limitations to protect the individual interests of a (potential) litigant, Article 23(1)(f) GDPR allows limitations to protect the court proceedings themselves as well as the applicable procedural rules.

3.4 Data subjects' rights and controller's obligations which may be restricted

35. In accordance with Article 23 GDPR, only Article 5 as far as its provisions correspond to the rights and obligations provided for in Article 12 to 22, Articles 12 to 22 and 34 GDPR can be restricted. The restrictions to obligations regard restrictions to the principles relating to the processing of personal data as far as its provisions correspond to the rights and obligations provided in Article 12 to 22 GDPR and to the communication of a personal data breach to the data subjects . Article 5 GDPR, which establishes the principles relating to the processing of personal data, is one of the most important articles in the GDPR. Restrictions to the data protection principles need to be duly justified by an exceptional situation, respecting the essence of the fundamental rights and freedoms at issue and following a necessity and proportionality test. It should be noted that Article 5 GDPR can be only restricted in so far as its provisions correspond to the rights and obligations provided in Articles 12 to 22 GDPR.

36. The restrictions to rights concern the right to transparent information (Article 12 GDPR), right to information (Articles 13 and 14 GDPR), right of access (Article 15 GDPR), right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR), right to restriction of processing (Article 18 GDPR), notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19 GDPR), right to data portability (Article 20 GDPR), right to object (Article 21 GDPR), right not to be subject to an automated individual decision making (Article 22 GDPR).

37. This means that any other data subjects' rights - such as the right to lodge a complaint to the supervisory authority (Article 77GDPR) - or other controllers' obligations cannot be restricted.

3.5 Necessity and proportionality test

38. Restrictions are only lawful when they are a necessary and proportionate measure in a democratic society, as stated in Article 23(1) GDPR. This means that restrictions need to pass a necessity and proportionality test in order to be compliant with the GDPR[13].

39. The objective of general interest provides the background against which the necessity of the measure may be assessed. It is therefore important to identify the objective of general interest in sufficient detail so as to allow the assessment on whether the measure is necessary. For example, if in administrative proceedings it is necessary to restrict part of the investigation, but some information can already be disclosed to the data subjects concerned, then that information should be provided to the person. The case law of the CJEU applies a strict necessity test for any limitations on the exercise of the rights to personal data protection and respect for private life with regard to the processing of personal data: 'derogations and limitations in relation to the protection of personal data (...) must apply only insofar as is strictly necessary'[14]. The ECtHR applies a test of strict necessity depending on the context and all circumstances at hand, such as with regard to secret surveillance measures[15].

40. If this test is satisfied, the proportionality of the envisaged measure will be assessed. Should the draft measure not pass the necessity test, there is no need to examine its proportionality. A measure which is not proved to be necessary should not be proposed unless and until it has been modified to meet the requirement of necessity.

41. The necessity and proportionality test will typically imply assessing the risks to the rights and freedoms of the data subjects. The risks to the rights and freedoms of data subjects will be detailed in point 4.7 of this guidelines.

42. According to the proportionality principle, the content of the legislative measure cannot exceed what is strictly necessary to safeguard the objectives listed in Article 23(1)(a) to (j) GDPR. The general public interest of the restriction must therefore be appropriate for attaining the legitimate objectives pursued by the legislation at issue and not exceed the limits of what is appropriate and necessary in order to achieve those objectives. According to the CJEU case law, Article 23 GDPR cannot be interpreted as being capable of conferring on Member States the power to undermine respect for private life, disregarding Article 7 of the Charter, or any of the other guarantees enshrined therein. In particular, the power conferred on Member States by Article 23(1) GDPR may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary[16].

---

[13] Within the mission of the supervisory authorities and in order to ensure legal certainty it is advisable that the proportionality and necessity test is documented. Supervisory authorities may request additional documentation.

[14] See CJEU, judgment of 16 December 2008, case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, ECLI:EU:C:2008:727, paragraph 56.

[15] See ECtHR, Szabo and Vissy v. Hungary, 12 January 2016, paragraph 73.

[16] CJEU, judgment of 6 October 2020, La Quadrature du net and others joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, paragraph 210. For example, in relation to data retention by online public communication services and hosting services providers, the CJEU concluded, paragraph 212, that "Article 23(1) (GDPR), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services".

43. A proposed restriction measure should be supported by evidence describing the problem to be addressed by that measure, how it will be addressed by it, and why existing or less intrusive measures cannot sufficiently address it. There is also a requirement to demonstrate how any proposed interference or restriction genuinely meet objectives of general interest of the State and EU or the need to protect the rights and freedoms of others. The restriction of data protection rights will need to focus on specific risks.

44. For example, if restrictions contribute to safeguarding public health in a state of emergency, the EDPB considers that the restrictions must be strictly limited in scope (e.g. as to the purpose, data subject rights concerned or the categories of controllers concerned) and in time. In particular, it must be limited to the emergency state period. Data subject rights can be restricted but not denied.

4 REQUIREMENTS OF ARTICLE 23 (2) GDPR

45. According to the CJEU case law, any legislative measure adopted on the basis of Article 23(1) GDPR must, in particular, comply with the specific requirements set out in Article 23(2) of the GDPR.[17] Article 23(2) GDPR states that the legislative measures imposing restrictions to the rights of data subjects and the controllers' obligations shall contain, where relevant, specific provisions about several criteria outlined below. As a rule, all the requirements detailed below should be included in the legislative measure imposing restrictions under Article 23 GDPR.

46. Exceptions to this rule, based on the fact that one or more provisions in Article 23(2) GDPR are not relevant regarding the legislative measure foreseeing the restriction of data subjects' rights, need to be duly justified by the legislator. The EDPB's interpretation of the expression "where relevant" in Article 23 (2) GDPR is linked to the circumstances.

47. Article 23(2)(a) GDPR mentions the purposes of the processing or categories of processing as one of the specific provisions that shall be mentioned in any legislative measures restricting the rights of data subjects or controllers' obligations. As per Recital 8 GDPR, the reason for the restriction should be comprehensible to persons to whom it applies. This also involves a clear understanding of how and when the restriction may apply.

48. For example, national legislation on prevention and investigation of breaches of ethics for regulated professions might state that if the disclosure of the fact that a person is under investigation for a serious breach may be prejudicial to the purpose of the investigation, the information may not be disclosed to the data subject for a limited time.

49. The possible purposes of the processing need to be linked to the grounds of the restrictions mentioned in point 3.3 of these guidelines.

50. It should be said that sometimes the exercise of data subjects' rights helps the controllers performing their function. For example, the right to rectification can contribute to the quality of the data.

4.1 Categories of personal data

[17] CJEU, judgment of 6 October 2020, La Quadrature du Net and others joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, paragraph 209.

51. Article 23(2)(b) GDPR states that the categories of personal data involved in restrictions are to be indicated in the legislative measure foreseeing those restrictions[18].

52. In the same vein, restrictions entailing special categories of personal data may have a bigger impact on the data subjects and, therefore, the legislative measure setting such a restriction should mention the special categories therein involved.

4.2 Scope of the restrictions

53. Article 23(2)(c) GDPR prescribes that the scope of the restrictions shall also be specified, i.e. which rights are concerned and how far they are going to be limited, for instance, that a restriction only concerns the right to restriction of processing (Article 18 GDPR), or that it may concern access, rectification and confidentiality of communication.

4.3 Safeguards to prevent abuse or unlawful access or transfer

54. Article 23(2)(d) GDPR states that the legislative measure shall include safeguards to prevent abuse or unlawful access or transfer. This refers in particular to organisational and/or technical measures[19] which are necessary in order to avoid breaches or unlawful transfers such as the storage in a safe way of physical documents. For example, in some Member States the exercise of rights in respect of processing carried out in specific sectors can be exercised through the mediation of the national SA.

55. The legislative measure may also concern periodic measures to review a given decision on restrictions. The legislator may propose that each restriction implemented by the controller should be reviewed periodically to ensure that the justification for it is still valid.

4.4 Specification of the controller

56. Article 23(2)(e) GDPR requires that the legislative measure specifies who the controller is or who the categories of the controller are. This appointment of the controllers in the legislative measure not only favours legal certainty regarding the responsibility for the processing operations in relation to the restrictions, but also will allow data subjects to know whom to address when exercising their rights, once the restriction is lifted.

4.5 Storage periods

57. Article 23(2)(f) GDPR establishes that the legislative measure must include a specific provision regarding the storage periods and applicable safeguards taking into account the nature, scope and purposes of the processing/categories of processing. For instance, the retention period could be calculated as the duration of the processing operation plus additional time for potential litigation.

4.6 Risks to data subjects' rights and freedoms

58. Article 23(2)(g) GDPR requires that the legislative measure include the risks to data subject's rights and freedoms entailed by the restrictions. This is a very important step, which helps in the necessity and proportionality test of the restrictions.

59. The goal of this assessment of the risks to data subjects' rights and freedoms is twofold. On the one hand, it provides an overview of the potential impact of restrictions on data subjects. On the other

[18] Where possible, the controller can go further and list the specific data items to which the restriction of rights may apply, such as the preliminary results of an investigation, a decision opening an inquiry, etc.

[19] See EDPB Guidelines 4/2019 on Article 25 data protection by design and by default, available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

hand, it provides elements for the necessity and proportionality test of the restrictions. In this regard and if applicable, a data protection impact assessment should be considered.

60. The legislator should assess the risks to data subject's rights and freedoms from the perspective of the data subjects. It is not always mandatory to perform a DPIA, but concrete risks to data subjects - such as erroneous profiling leading to discrimination, reduced human dignity[20], freedom of speech, the right to privacy and data protection[21], a bigger impact on vulnerable groups (such as children or persons with disability), to mention a few - may be stated in the legislative measure, if applicable.

61. When such assessment is provided, the EDPB considers necessary to include it in the recitals or explanatory memorandum of the legislation or in the impact assessment[22].

4.7 Right to be informed about the restriction, unless prejudicial to the purpose of the restriction

62. Article 23(2)(h) GDPR states that, unless it may be prejudicial to the purpose of the restriction, data subjects shall be informed of the restriction. This means that data subjects should be informed about the restriction to their right to information as a rule. To that purpose, a general data protection notice may be sufficient.

63. For example, where a data subject specifically asks to exercise a particular right at a very delicate moment of a given administrative investigation, the data subject should, if possible, be informed of the reasons for the restriction. However, if informing the data subject of the reasons for the restriction would result in cancelling the effect of the restriction (i.e. would hamper the preliminary effects of the investigation), that information may not be disclosed. Restrictions may be adopted to protect investigations. In this case, restrictions must remain necessary and proportionate and to do so an assessment should be performed by the controller to check whether informing the data subject of the restriction is prejudicial to the purpose of the restriction.

64. In other words, in extraordinary circumstances, for instance in the very preliminary stages of an investigation, if the data subject requests information if he or she is being investigated, the controller could decide not to grant that information at that moment - if this restriction is lawful and strictly necessary in the specific case it where prejudicial to the purpose of the restriction.

65. At a later stage, such as after the preliminary phase of the investigation or inquiry is completed, data subjects should receive a (specific) data protection notice. It is still possible at this stage that certain rights continue to be restricted, such as the right of access to the information about the opening an investigation, or to the allegations of potential victims of harassment[23]. This fact should be indicated in the data protection notice along with an indication of a period in which the rights will be fully restored, if possible.

[20] Human dignity is a right protected by Article 1 of the Charter.
[21] Articles 7 and 8 of the Charter.
[22] See Article 35 (10) GDPR.
[23] For further information, see CJEU, judgment of 17 July 2014, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, cases C-141/12 and C-372/12, ECLI:EU:C:2014:2081, paragraphs 45 and 46 and judgment of 20 December 2017, Novak, case C-434/16, ECLI:EU:C:2017:994, paragraph 56.

5 ACCOUNTABILITY PRINCIPLE

66. In light of the accountability principle (Article 5(2) GDPR), the controller should document the application of restrictions on concrete cases by keeping a record of their application. This record should include the applicable reasons for the restrictions, which grounds among those listed in Article 23(1) GDPR apply (where the legislative measure allows for restrictions on different grounds), its timing and the outcome of the necessity and proportionality test. The records should be made available on request to the data protection supervisory authority (SA).

67. In case the controller has a data protection officer (DPO), the DPO should be informed without undue delay whenever data subject rights are restricted in accordance with the legislative measure. The DPO should be given access to the associated records and any documents concerning the factual or legal context in which the restriction takes place. The involvement of the DPO in the application of restrictions should also be documented.

6 CONSULTATION WITH THE SAS (ARTICLES 36(4) AND 57(1)(C) GDPR)

68. In accordance with Article 36(4) GDPR, where restrictions are adopted at the level of the Member States, SAs shall be consulted before the adoption of the legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure envisaging the restriction of data subjects' rights under Article 23 GDPR.

69. Also, it is within the tasks of the SAs to provide advice on legislative measures relating to the protection of individuals' rights and freedoms regarding their personal data processing, in accordance with Article 57(1)(c) GDPR.

70. If SAs are not duly consulted, they can issue under Article 58(3)(b) GDPR on their own initiative opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions or bodies as well as to the public on any issue related to the protection of personal data.

71. At that stage and if applicable, the SAs may ask for a data protection impact assessment (DPIA) under Article 35 GDPR. That assessment will be helpful in the description of the risks to the data subjects' rights mentioned above in point 4.6.

72. In addition, data protection legislation at national level may set out specific procedures regarding the adoption of legislative measures that aim at restricting the rights afforded by Articles 12 to 22 and Article 34 GDPR, in line with Article 23 GDPR. This could be the case only if in line with the GDPR.

7 EXERCISE OF DATA SUBJECTS' RIGHTS AFTER THE LIFTING OF THE RESTRICTION

73. The controller should lift the restrictions as soon as the circumstances that justify them no longer apply. If the data subjects have not yet been informed of the restrictions before that moment, they should be at the latest when the restriction if lifted.

74. During the application of a restriction, data subjects may be allowed to exercise certain rights, if not all their rights need to be restricted. In order to assess when the restriction can be partially or integrally lifted, a necessity and proportionality test may be performed several times during the application of a restriction.

75. When the restriction is lifted - which should be documented in the record mentioned in point 5 -, data subjects can exercise all their rights.

76. If the controller does not allow data subjects to exercise their rights after the restriction has been lifted, the data subject can submit a complaint to the SA against the controller, in accordance with Article 57(1)(f) GDPR.

8 INFRINGEMENTS OF ARTICLE 23 GDPR

8.1 Non-observation of Article 23 GDPR requirements by a Member State

77. The European Commission, as Guardian of the Treaties, has the duty to monitor the application of EU primary and secondary law and to ensure its uniform application throughout the EU, including by taking actions where national measures would fail to comply with EU law.

78. Furthermore, where the legislatives measures imposing restrictions under Article 23 GDPR do not comply with the GDPR, in accordance with Article 58(5) GDPR and where appropriate, SAs shall have the power to bring infringements of this Regulation to the attention of the judicial authorities to commence or engage otherwise in legal proceedings, in order to enforce the provisions of the GDPR.

79. According to the principle of supremacy of EU law, the "duty to disapply national legislation that is contrary to EU law is owed not only by national courts, but also by all organs of the State — including administrative authorities — called upon, within the exercise of their respective powers, to apply EU law"[24].

8.2 Non-observation of a legislative measure imposing such restrictions by a controller

80. Where the legislative measures imposing restrictions under Article 23 GDPR comply with the GDPR but are infringed by a controller, SAs can make use of their advisory, investigative, corrective and powers against it, as in any other case of non-observation of GDPR rules.

81. In accordance with the powers foreseen in Article 58(1) GDPR, the SAs have the following investigative powers:

- order the controller and the processor, and, where applicable, the controller's or processor's representative to provide any information it requires for the performance of its tasks;
- carry out investigations in the form of data protection audits;
- notify the controller or the processor of an alleged infringement of the GDPR;
- obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

[24] CJEU, judgment 4 December 2018, Case C-378/17, ECLI:EU:C:2018:979, paragraph 38.

82. If corrective measures need to be applied, the SAs can in accordance with Article 58 (2) GDPR:

- **issue warnings** to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- **issue reprimands** to a controller or a processor where processing operations have infringed provisions of the GDPR;
- **order** the controller or the processor **to comply** with the data subject's requests to exercise his or her rights pursuant to the GDPR;
- **order** the controller or processor **to bring processing operations into compliance** with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;
- **order** the controller **to communicate a personal data breach to the data subject**;
- **impose** a temporary or definitive limitation including **a ban** on processing;
- **order** the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 GDPR and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR;
- **impose an administrative fine** pursuant to Article 83, in addition to, or instead of measures referred to in Article 58(2) GDPR, depending on the circumstances of each individual case;
- **order** the suspension of data flows to a recipient in a third country or to an international organisation.

83. Regarding the SAs advisory powers foreseen in Article 58(3) GDPR, they can:

- advice the controllers in accordance with the prior consultation procedure referred to in Article 36(1) and (5) GDPR;
- authorise processing referred to in Article 36(5) GDPR, if the law of the Member State requires such prior authorisation.

9 CONCLUSIONS

84. Article 23 GDPR allows under specific conditions, a national or Union legislator to restrict, by way of a legislative measure, the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 GDPR in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, inter alia, important objectives of general public interest of the Union or of a Member State.

85. Restrictions of data subjects' rights need to observe the requirements stated in Article 23 GDPR. The Member States or the Union issuing the legislative measures setting those restrictions and the controllers applying them should be aware of the exceptional nature of these restrictions.

86. The proportionality test should be carried out before the decision-making of applying a restriction by the legislator.

87. SAs should be consulted before the adoption of the legislative measures setting the restrictions and have the powers to enforce its compliance with the GDPR.

88. Once restrictions are lifted, data subjects must be allowed to exercise their rights by the controller.

10 ANNEX: CHECK-LISTS - ARTICLE 23 GDPR IN A NUTSHELL

10.1 Requirements under Article 23(1) GDPR

i. *Respect of the essence of the fundamental rights and freedoms*
ii. *Proportionality and necessity test*
iii. *Legislative measures laying down restrictions and the need to be foreseeable (Rec. 41 and CJEU case law)*
iv. *Data subjects' rights and controller's obligations which may be restricted*
    a) the right to transparent information (Article 12 GDPR),
    b) right to information (Articles 13 and 14 GDPR),
    c) right of access (Article 15 GDPR),
    d) right to rectification (Article 16 GDPR),
    e) right to erasure (Article 17 GDPR),
    f) right to restriction of processing (Article 18 GDPR),
    g) notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19 GDPR),
    h) right to data portability (Article 20 GDPR),
    i) right to object (Article 21 GDPR),
    j) right not to be subject to an automated individual decision making (Article 22 GDPR)
    k) obligations provided in Article 12 to 22 GDPR (Article 5 GDPR) and
    l) the communication of a personal data breach to the data subjects (Article 34 GDPR)
v. *Grounds for the restrictions*
    a) national security;
    b) defence;
    c) public security;
    d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
    e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
    f) the protection of judicial independence and judicial proceedings;
    g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
    h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
    i) the protection of the data subject or the rights and freedoms of others;
    j) the enforcement of civil law claims.

10.2 Requirements under Article 23(2) GDPR

i. *the purposes of the processing or categories of processing;*
ii. *the categories of personal data;*
iii. *the scope of the restrictions introduced;*
iv. *the safeguards to prevent abuse or unlawful access or transfer;*
v. *the specification of the controller or categories of controllers;*

vi. *the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;*
vii. *the risks to the rights and freedoms of data subjects; and*
viii. *the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction*.